Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2002 Proceedings

Americas Conference on Information Systems (AMCIS)

December 2002

PRIVACY: A PHILOSOPHICAL, LEGAL, BUSINESS, AND TECHNICAL PERSPECTIVE

William Friedman
University of Central Arkansas

PRIVACY: A PHILOSOPHICAL, LEGAL, BUSINESS, AND TECHNICAL PERSPECTIVE

William H. Friedman
University of Central Arkansas
friedman@mail.uca.edu

Abstract

Privacy, while rarely a major social concern before 1900, has recently become a high profile issue, bordering on obsession for the general public as well as for the computer and the business worlds. Discussants of privacy rights often take much for granted, and in the most extreme cases, their assertions about privacy and rights are made in a tone of almost "axiomatic" self-certainty. They typically proceed with the full expectation that the intended audience will assent to the spokesperson's positions without question. There have been many proposed and actual extensions of the scope of privacy, which have now progressed to demands for shielding virtually all information about anything an individual might wish to keep secret, despite the existence of reasonable, competing values. For example, in the US, a student has a legal right to keep his/her parents, whether they defray the student's tuition or not, from ever learning from a university that the student has failed every course.

The most common starting point for discussions on privacy is that it is a natural, inviolable right as well as an important value. When a value-laden policy position has attained such unquestioned influence, it is both appropriate and timely to examine critically the extent of its applicability and whether it in fact embodies the overarching values (Gurak 2002) attributed to it. This paper attempts just such an analysis from an information technology, business, social, legal, and philosophical perspective. The values competing with privacy and the matter of the origins of privacy and other rights play a central role in this analysis.

Keywords: Privacy, philosophy, law, surveillance, information technology

*A cartoon by Casey Shaw displayed a sign over the counter in a pub: "Welcome to **Cheers** 2002, A Cyber Café." Every customer was surfing the web on PCs, apparently attached to a single server. The cartoon caption (relevant to this paper) was a takeoff on the **Cheers** theme song: "Where everybody knows your name … and your address, age, and purchasing preferences." USA Weekend, 3-10-2002*

What Is Privacy?

It is useful to consider three definitions of *privacy,* which give the range of common usages and, therefore, will be used to set the parameters for this paper. The original meaning was apparently a notion like "the quality or state of being apart from company or observation" and then came to mean "freedom from unauthorized intrusion." (Britannica & Merriam-Webster's Collegiate Dictionary 1997). Several interesting philosophical questions are suggested by these definitions. One should notice that the first definition emphasizes the actions and desires of a person secluding him/herself, and the outsider is regarded as having the role of passive observer. There is even the possibility that the privacy seeker is unaware of being observed. The second definition, however, views the outsider as actively disturbing the privacy seeker without authority or invitation. A physical intrusion, of course, does not usually go unnoticed. The question of what is the "authority" for the intrusion raises some important issues. Is it the authority of the privacy-seeker that is involved or perhaps some governmentally sanctioned intrusion? Is the latter justifiable? Are we to extend or understand the second definition also to include intrusions not noticed by the privacy seeker, say surreptitious scanning of his/her computer files (Brandt 2001). Is the harm greater if one notices the intrusion only after the fact? Does the harm derive only from the intruder's causing pain or damage to the person whose privacy is invaded?

A third definition from another source (QPB Dictionary of Ideas 1996) states that privacy is "a right of the individual to be free from secret surveillance (by scientific devices or other means) and from the disclosure to unauthorized persons of personal data, as accumulated in computer data banks." This definition introduces additional, very important considerations, especially in light of the questions raised in connection with the previous definitions:

(a) Surveillance, not merely observation—the implication here is that there is a more constant observation with a definite purpose,

(b) Disclosure of what is observed (personal data) to unauthorized persons—still, however, leaving open the question of who gives the authorization, and

(c) Computer banks—as if other means of storage, like hard copy dossiers, are not of such great consequence now. Undeniably, what makes "computer banks" so crucial to any discussion of privacy is that they involve rapid collection, storage, retrieval, and dissemination. Additionally, the computer provides for such activities on a massive scale and often in hard to detect ways.

First Philosophical Consideration: Is Privacy a Natural Right?

People often unconsciously create, out of their personal desire for something or very strong feelings about something, a right with respect to that something. More often than not, they would go further and "find" that "right" in a Platonic realm of ideas or, via a more sophisticated flourish, they might claim knowledge of that right through an *a priori* (hence, they believe, infallible) intuition. If such claims were to go unchallenged, they might assert more rights than we could ever imagine, no doubt all of them would also be metaphysically derived. Furthermore, those making such assertions could claim entitlements to all sorts of things and for all sorts of entities, perhaps even for inanimate entities like deserts, which, some environmentalists might one day say, literally have a "right" to be left alone and remain unspoiled.

Among those discussing privacy, there are many professed sources of ideas about the origins and authority for rights and privacy, such as divine revelation, superior understanding, legal traditions, or even empirical investigations. Aquinas for one refers to an "eternal law" or natural law imprinted on all creatures; and it is our rationality that gives us access to these laws about proper behavior. Whatever the claimed source, it would still be beneficial to be able to construct arguments that seem coherent, if not always convincing, to others not necessarily sharing the same (frequently) unquestioned starting points. The aim advanced here, then, is to find a common ground from which to start--one that might even lead to the same conclusion that others have reached, even though they might start out from totally different initial presuppositions. On the assumption that the ultimate goal of a privacy advocate is purely practical, perhaps to enact legislation and construct guidelines, it would certainly be more effective and more efficient to avoid appeals to one's own source of "the truth" to justify these practical ends. Rather than try to change another person's basic metaphysical and ethical outlook, one should try to use reasons acceptable to the other person to arrive at the desired practical outcome.

A partisan of natural law, of course, assumes that his/her notions of privacy are common to all humankind. A proponent of positive law, on the other hand, would say that laws of privacy are the product of human action and are legitimately imposed by the society on itself. Aquinas also provides for human or positive law, "which must be framed by human societies to achieve the order and peace needed for perfection" (Beck 1979). It will be an important part of this paper to deal with inner peace and diminishment of anxiety due to privacy concerns.

Any society wishing to create privacy laws should, however, be ready to attempt to justify its privacy proposals on grounds acceptable to all parties, irrespective of their views on the nature and source of law, and even to skeptics of the need for such legislation. One way to reach a practical consensus among parties with widely differing views on what makes rights and laws valid is to stipulate, that rights and laws exist to make society function more smoothly and to ensure that the people will be secure and relatively happy. After all, no advocate can consistently contend that nature (or whatever is the source of rights) could be wrong about what is best for society. Even proponents proceeding from absolute metaphysical first principles would find comfort in thinking that their metaphysical beliefs were confirmed by pragmatic and empirically verified success. Empirical verification of what society wants and needs can be obtained from surveys, referenda, communications to and selection of political and judicial representatives.

Thus, the initial philosophical conclusion of this paper is that when establishing privacy rights, they should be considered as stemming from and should conform to an empirical determination of society's wishes and its psychological well-being. The ensuing rights and laws are to be maintained and observed only insofar as they promote both the general and individual welfare and only when they facilitate societal functioning. The smoothness of societal functioning can be evaluated by experimental means. A balance between general and individual welfare is also a prime goal. Privacy laws are normally desired to prevent harm and general anxieties in the population. Claims to privacy are to be granted unless there are supervenient circumstances. If overriding circumstances like threat of terrorism arise, the degree of reduction in the right to privacy should be decided by the society in danger. Thus reliance on democratic and empirical processes will be more likely to garner popular support than rigid reliance on absolutes derivable from sources not universally accepted.

The Evolution of Privacy as a Legal Right

The US Constitution is often a starting point in discussions of privacy. It does not explicitly mention a legal right to privacy, but such a right is traditionally considered to have been created by the first, fourth, and fifth amendments to this constitution (Blumenfeld 1998). The fourth amendment prohibits unreasonable searches and seizures; the other two, however, concentrate on the citizen's freedom to feel secure from arbitrary governmental acts. The Fifth Amendment says: "nor shall private property be taken for public use, without just compensation;" but here the concern is with justice, not privacy. The First Amendment does not really vouchsafe privacy in any of the senses mentioned earlier; rather it guarantees free speech, free exercise of religion and freedom to assemble. However, in this author's view the third amendment is also quite relevant to privacy. It assures that no soldier will be forcibly introduced into a citizen's household, thereby guaranteeing not to disturb "the quality or state of being apart from company or observation."

In many western countries the right to privacy is derived from tort law, where it seems to have originated in the 19th century: (Britannica 1997)

> Subject to limitations of public policy, it asserts a right of persons to recover damages or obtain injunctive relief for unjustifiable invasions of privacy prompted by motives of gain, curiosity, or malice. In torts law, privacy is a right not to be disturbed emotionally by conduct designed to subject the victim to great tensions by baring his intimate life and affairs to public view or by humiliating and annoying invasions of his solitude.

(a) Chief Judge Alton B. Parker of the New York State Court of Appeals decided in Roberson vs. Rochester Folding Box Co. in 1901 that

> "a man has a right to pass through this world, if he wills, without having his picture published, his business enterprises discussed, his successful experiments written for the benefits of others, or his eccentricities commented upon, whether in handbills, circulars, catalogues, newspapers, or periodicals." (Helm 2000, p. 204)

This opinion has, of course a direct bearing on privacy discussions today. No doubt, Judge Parker would add electronic media to his list. It seems he might also have wished to amend his decision by writing that "A man with no allegations of criminal intent against him has a right to pass through this world …." Were this not so, violent criminals, political terrorists, certain Enron officials, and the like would be exempt from bad publicity and even publicly displayed "wanted" posters.

(b) Associate Justice of the US Supreme Court, Louis D. Brandeis, was a forerunner in the advocacy of a legal foundation for privacy when he wrote in a dissenting opinion in 1928 case about governmental wiretapping to entrap a bootlegger. It is remarkable for its prescience in dealing with as yet unknown technologies:

> "The progress of science in furnishing the government with means of espionage is not likely to stop with wire tapping. Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court…
>
> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness…. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations…The principle most often quoted from this paragraph by Brandeis continues:

> "They conferred as against the government, the right to be let alone—the most comprehensive of rights and the right most valued by men."

This is significant because it concerns the psychological sense of privacy (as defined previously, the quality or state of being apart from company or observation), but even though it dealt with the least controversial sense of privacy it was part of in an uphill battle for privacy protection--for it appeared in a dissenting opinion, Olmstead vs. U.S., June 4, 1928. Even earlier, in 1890, Brandeis and Samuel Warren had advocated privacy rights and personal autonomy in an influential article, "The Right to Privacy," published by the Harvard Law Review. However continuing (in that same opinion), Brandeis also wrote about the second, physical sense of privacy (freedom from unauthorized intrusion):

> "To protect that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment."

The limitation of this opinion to governmental action does not yet relate to privacy violations by non-governmental agents, let alone computer bots.

(c) In 1967, the US Freedom of Information Act (FOIA) established the rights of citizens and organizations to examine unclassified files kept by the executive branch of the government. While there is potential for abuse and for misclassifying totally innocuous information (i.e., information not proper to keep secret), this exception for classified material was obviously designed to protect the society as a whole from its enemies. The FOIA specifically exempts

> "records that relate to national security, internal agency personnel matters, trade secrets which [sic] have been given to the government by businesses, advice and recommendations on government policies written by government employees, personal privacy matters such as health records, law enforcement investigations, federally regulated banks and oil and gas well records. However, generally these exemptions are not absolute." (Helm 2000, p. 481)

The purpose of this act is ostensibly to protect citizens by informing them of what is known about them, but, ironically, it reduces their privacy by making it easier for third parties to know what the government has uncovered about any citizen. Access can be limited to certain individuals, e.g., those who can "demonstrate" a public interest in knowing, but the amount and likelihood of undesired disclosure have still been increased by this law. Moreover, this law does not (Helm 2000, p. 479) pertain to data kept by Congress, federal courts, private corporations, or state and local governments, though several states have remedied the situation about their own records. Finally, the law does not limit what type of information can be collected.

The issue of whose privacy is preeminent can arise in any arena with conflicting interests. One such instance occurred when the US Environmental Protection Agency discovered that radioactive tailings were used as fill during home construction in Colorado. The EPA wanted to withhold the names and addresses of the homeowners involved based on the exemption about personal information in the FOIA. However, the real reason for withholding the information apparently was that it was afraid the homeowners would be unduly frightened to learn which of them had radioactive materials in their house foundations. A Court of Appeals ruled against the concealment saying it would cause more fear if the homeowners did not know. Other problems would arise if prospective new buyers of these homes were not aware that they might buy radioactive property from existing owners. Could existing homeowners rightfully complain of privacy violations and that deleterious effects on resale value would be incurred if information about which homes were radioactive were made available on the web? This is not merely a case where sellers would knowingly sell defective property, but where privacy would have "protected" the sellers from knowing.

(d) The US Privacy Act of 1974 has three important provisions: that there be no secret data banks, effort must be made to see that the data are reliable, and the information cannot be used for a purpose different from the original reason for collecting it.

Two issues of interest to both lawyers and information system professionals are explicated by the Privacy Act. What exactly is a record? It has three components:

i. It must contain personal information
ii. One must be able to locate it by searching for it by using either the person's name or social security number, and
iii. It must be under an agency's control.

What are the data integrity requirements of personal information? Data must be accurate, relevant, timely and complete." A citizen should be allowed to correct the records with sufficient proof. (Helm 2000, p. 482) Thus if the information is no longer concealed, at least what can be revealed will be correct.

(e) In the UK, the Data Protection Act of 1984 assures the citizenry by requiring a registry of all organizations collecting and processing personal data. Moreover, there are standards of propriety set forth in the law. (QPB Dictionary of Ideas 1996) Clearly, this law gives the green light to any organization that might have hesitated (for reasons of lawsuits, for example) to collect personal data, but now indirectly finds it legal to do so. One wonders if the general level of privacy has been increased. Perhaps in the sense of being left alone, the standards contained in this law will help.

(f) In the US but not the UK, there are some restraints on the media (and by extension the Internet) invasion of personal privacy: the operative rule is that only those in public life ("politicians, entertainers, and athletes") can have their private information made public (QPB Dictionary of Ideas 1996). This noteworthy exception raises the question: what moral justification is there that such people are excluded from the protection afforded everyone else?

Why Do Individuals Care about Their Personal Privacy?

Individuals perhaps associate privacy with freedom, if not as identical concepts, at least as closely dependent rights. Some of the key desires for and effects of privacy might be listed before proceeding:

(a) Tranquility, freedom from unwanted intrusion.

(b) Hope to avoid embarrassment over the privacy seeker's activities, if not socially acceptable.

(c) Endeavor to avoid economic harm, say, through stealing of identity or credit card numbers, job discrimination, etc.

(d) Endeavor to avoid criminal harm. Miscreants might, through eavesdropping, learn that a house is unoccupied or occupied by a frail older woman.

(e) General uneasiness about having others know our business.

(f) Shyness about being the subject of other's conversation, even if nothing embarrassing was done.

(g) Desire to avoid unwanted contacts initiated by others seeking social contact, e.g., movie stars.

(h) Desire to avoid stalkers or other types of predators.

(i) Desire to avoid being made to fulfill responsibilities, e.g., dead-beat dads avoiding child-care payments.

(j) Desire to conceal crimes or actions outside the community's standards of behavior, if not of themselves illegal behavior.

In this list, there are commendable, neutral and, one could fairly say, desires antithetical to the common welfare. Many of the above concerns stem from persons wishing to hide certain behaviors not harmful to others for fear of incurring discrimination, censure, or other unwanted consequences. When it is better understood that some behavior we wish to keep secret is actually widely practiced, there will be less anxiety over both engaging in that behavior and being discovered through a breach of privacy. Thus the right to privacy tends to perpetuate anxiety over behavior and fear of being discovered. Furthermore, the very possibility of privacy tends to enable hypocritical condemnation of some behaviors, since there is no way of knowing that the hypocritical blamer is engaged in the same activity.

What Conditions Justify a Violation of Privacy, If Any?

Commonly offered reasons include:

(a) Government need such as law enforcement or tax collection

(b) Protection of a society's security or apprehension of criminals. Police may need to invade privacy "for the greater societal good."

(c) Security of someone under the control of a surveilled person. If society suspects a controller of child or spousal abuse, invasion of the controller's privacy to protect the victim—of course, with a warrant seems justifiable, depending on the evidence.

(d) Sometimes privacy concerns are innocently overridden by business interests. Keeping track of consumer choices to plan how to serve him/her more efficiently. One example of this is for a web service to maintain lists of a customer's frequently visited URL's or even cached copies of entire Web pages on proxy servers to hasten load times. Clearly, this involves unexpected and unwanted disclosures. Should this be stopped or should we just install adequate safeguards, e.g., make it impossible to trace specifically who made the choice and then record only general impersonal attributes of the choice, like the date an item was purchased, the web site visited, etc.? Comcast, a popular cable company had been using Inktomi software for this purpose. Its customers became aware of the practice and complained. One of the complaints was that the information garnered might be used for law enforcement purposes. (Cowley 2002)

What Are Commonly Cited Justifications for Requiring That Others Guard Our Privacy?

(a) For an organization, respect for privacy would be necessary to retain the confidence of its present clients, though the obligation might be expected to continue after a person ceased having that status. Naturally, not to safeguard private matters would invite lawsuits, so there is a financial incentive as well.

(b) An organization or company is usually *expected* to safeguard and not to intrude on the private matters of employees. However, the legal standing of this expected "right" is very weak, the US law gives preference to the needs of the employer to know about the employee and his/her activities, especially on the job (Friedman 2000).

(c) We surrender many liberties and facts about ourselves to the government. In the final analysis, this is should only be for the sake of physical protection; we expect that private matters about ourselves not be made known to third parties without our explicit authorization. An example of government's deriving profit from selling private information occurs when states sell drivers license information to automobile insurance companies. If the government claims that its selling of personal information brings in needed revenue and reduces taxes, any concerned citizen should insist that the release of one's personal information be contingent on explicit permission of the citizen. Furthermore, the reason for supplying personal information is not governmental profit-making. However, the citizenry should expect to bear the burden of extra taxation to compensate for revenue shortfalls when the government cannot sell personal information.

What General Welfare Interests Are Served by Exceptions to Privacy?

(a) Aids law enforcement. The US Constitution requires a judicially (if not always a judiciously) issued warrant before police can perpetrate obvious breaches of privacy like invading one's home.

(b) Computer (or any other type of) monitoring and targeting of consumers. These practices might lead to a greater quantity of desired products coming to market, in the right places, at the right times and at favorable prices, thus advancing commerce and benefiting consumers. Many businesses are "investing heavily in the ability to collect and leverage information in a wide range of ways that will produce benefits for both business and customer. (Cabral 2001) Still, despite any perceived benefits, customers are worried about who can access their information, what exactly is stored, how to keep it safe, and whether companies will sell or share it. The level of detail in collected information ought also to be a concern. "Data enhancement" is the practice of collecting individual, household and business level (as opposed to aggregate/market level)" information. (Hamilton 2001). An anonymous wit once remarked, "In the computer age it is disturbing to realize that a machine has your number."

(c) OLAP (online analytical processing) is software that allows vendors to analyze information that has been encapsulated into multidimensional views and hierarchies. OLAP places the data into a conceptual cube structure that can be rotated by the market analyst to obtain different perspectives. Such tools can be used to perform trend analysis on sales and customer

characteristics. They can enable vendors to sift through masses of sales data in order to isolate the products that are the most popular and for whom.

(d) When a person uses the Internet, he/she is presented with many unwanted advertisements, which can be very annoying. One IT company, DoubleClick, incurred almost universal wrath because it thought tracking the shopping habits and the web sites people visited would enable the sites to tailor advertisements to the visitors' real interests. At first glance, this activity seemed to make winners out of all concerned: vendors would gain efficiency in showing ads to the most probable customers and the web user would primarily see ads relevant to his/her own interests. The whole plan was scuttled, however, (Gurak 2002) perhaps because of disproportionate privacy concerns. The European Union passed an "EU data directive" to the effect that "when you are doing business over the Internet with a citizen of the EU, you're not allowed to collect and use their [sic] personal data without their permission" (Gurak 2002). Many US companies, perhaps in an endeavor to head off governmental regulation, voluntarily offer web site visitors the opportunity to opt out of being tracked or targeted by commercial emails, etc.

(e) While data mining and OLAP enhance the efficiency of commerce, the safest route for a business is the one that provokes the least controversy: just collect information without there being any possibility of associating such things as Internet surfing or buying trends with an identifiable individual. There are even objections to being targeted for special marketing felt by particular groups. A recent study showed that the Jewish community as a whole preferred not to be targeted as such (Demirdjian 2001).

Should Technological Devices Used for Privacy Penetration Be Prohibited?

There are many hardware and software technologies that can be used for abridging privacy. One such technology, key logging, has already become the subject of intense policy debate. What is said about this technique can be representative of what might be said about the entire category of eavesdropping, including wiretapping, and the like.

The US Federal Bureau of Investigation plans to develop and eventually implement a key logging technology known as "Magic Lantern." The full facts surrounding this project are still secret, but from several sources one can conclude that the

> "software would let the FBI send criminal suspects an email note with an attachment that, if opened, would insert a Trojan horse. Reports say users would activate the Trojan horse and its key logging capabilities if and when they launch Pretty Good Privacy encryption software. When the user types the password, Magic Lantern software would capture it, giving the agency the ability to decrypt users' communications." (Paulson 2002)

There are several caveats here. Would the FBI have to intrude into someone's home to deploy Magic Lantern? Probably a warrant would have to be issued under present law to do that, so the general (innocent) population would have little to fear, provided there are no abuses! Now some innocuous, but cautious users presently employ encryption, say, to ensure business privacy. Suppose a cracker (i.e., a criminal hacker) were to discover Magic Lantern software on a computer probed by the FBI. Then even the protection afforded by encryption software, e.g., Pretty Good Privacy, could be rendered ineffective.

Final Philosophical Discussion and Recommendations

(a) This author proposes a fairly uncontroversial principle namely that rights, when granted at all, should be fairly distributed. However, at present we countenance totally unwarranted exceptions to this principle: public figures are not legally entitled to the same privacy protections that the general population enjoys. Why are celebrities not afforded the same privacy privileges as others? Would it be right to "key snoop" or otherwise eavesdrop on celebrities when it is not right to eavesdrop on the general population? Why should those who practice a public profession pay a higher price in terms of surrendering their privacy rights? Do we justify this sacrifice of privacy as a perverse compensation to the rest of us, because we do not enjoy the emoluments of public recognition and acclaim? This is particularly unjust when the persons who are celebrities provide some sort of extraordinary benefit for the rest of us, in terms of entertainment or public service.

(b) As adumbrated previously, rights should be argued for and formalized on the basis of maintaining a tranquil and psychologically healthy society, since that would be more susceptible to corroboration than metaphysical appeals. Further, the right granted by society should not be regarded as absolute and indefeasible, because there can be extenuating

circumstances. There are tradeoffs with regard to privacy rights: perhaps some loss of privacy for some measure of security, degrees of applicability.

(c) Perhaps there is no right to privacy. A famous libertarian thinker wrote:

> "There can be no such thing as a privacy right in libertarianism, for under that philosophy, rights can never conflict. But your (so called) right to privacy conflicts with my right to take a picture of you, look at you, look up your records, be a detective assigned to follow you around, etc." (Block 2002)

The stance of this paper is that rights should be regarded as granted by authorized designees of a society, like the founding fathers of the American Constitution. It may very well be that the very human grantors have provided for rights that conflict. Even the conflicting rights cited by Block can be given degrees of applicability. For instance, person A could look at person B (who, incidentally, is free to wear a disguise) in public places, but not to surveill via electronic snooping (that picks up computer signals from B's home), unless there is a judicial warrant authorizing such. Well-defined boundaries can leave ample scope for all legitimate rights that society requires.

(d) Occasionally, commentators on societal issues may imply that privacy is breached because it can be, almost as if there were some irrational drive to penetrate our private lives over and above security and commercial motives. In one paper, the authors (Griffin and Whitehead 2001) write:

> "This information-gathering goes on in all facets of our society; government agencies, health-care providers, financial institutions, schools, and commercial businesses all want to know our secrets.

While individuals may want to know our personal secrets, probably organizations are most interested in a broader understanding of the public at large. Marketers may want to know what we can be expected to buy, and somehow it does not sound so nefarious when expressed that way. Should other personal traits come to light in that endeavor, there will, of course, be personal anxiety among those studied, and every effort should be made to reduce that anxiety and its causes. These authors go on to cite (without apparently endorsing) this defense of information gathering: "It creates a society that is closely linked and better informed."

If members of society could learn to feel that way, anxiety about privacy and hypocritical pronouncements on harmless behaviors would be considerably diminished. Further, if members of society would learn to tolerate what such information gathering reveals about other people, and upon realizing that there are many others who behave like themselves, they would in turn be tolerant of others and less upset when previously guarded behavioral facts about themselves become known. Naturally, we have not reached this condition of mutual toleration and understanding yet, and we still have to be on guard lest psychological, financial, and other types of harm come to us through breaches of our personal privacy.

A prime concern to the MIS and general business community is how to balance employee desire for privacy with protecting the organization. "The level of privacy to be extended to employees is a corporate philosophical decision that should start at the Board level and be filtered through all levels of the organization" (Griffin 1998). This answers the question of how rights could be developed in addition to surveys (methodologies for doing this in a sophisticated manner are well known), communities making their wishes known to legislators, even polls and letters to the editor. When government, the computer industry and corporations cooperate, we will arrive at levelheaded solutions that will protect the individual and encourage sustained growth in technology as well as commerce.

References

Beck, Robert. Handbook in Social Philosophy, New York, New York: Macmillan Publishing Co., 1979

Blumenfeld, Elizabeth. Privacy please: "Will the Internet industry act to protect consumer privacy before the government steps in?" The Business Lawyer; Chicago; November 1998.

Block, Walter. Subject: "Privacy," Personal email, Fri, 8 March, 2002 09:37:47 –0600, "(CBA) WALTER BLOCK" WALTERBLOCK@cba.loyno.edu

Brandeis, Louis. J. U.S. Supreme Court, "Olmstead v. U.S., 277 U.S. 438 (1928) http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=US&vol=277&invol=438

Brandt, Andrew. "Should Your Boss be Allowed to Search your Hard Drive?" PC World, December 2001.

Britannica CD97, Includes Merriam-Webster's Collegiate Dictionary, tenth edition, 1997.

Cabral, Robert. "U.S. Banking--Financial Privacy," 2001 Hawaii Conference on Business, June 14 -17, 2001. CD-ROM Proceedings, file C.doc, p. C3. Honolulu, Hawaii, USA, Editor(s): Terry Gregson and David Yang.

Cowley, Stacy. "Chastened Comcast Will Stop Tracking Customer Web Use," February 13, 2002 12:07 pm PT, http://www.infoworld.com/articles/hn/xml/02/02/13/020213hncomcast.xml.

Demirdjian, Z. S. "The Jewish Subculture: The Elusive and the Elite Market," 2001 Hawaii Conference on Business, June 14-17, 2001. The abstract but not the entire paper, appeared in the CD-ROM Proceedings, file D.doc, p. D-49, Honolulu, Hawaii, USA, Editor(s): Terry Gregson and David Yang.

Friedman, William H., "Is the Answer to Internet Addiction Internet Interdiction?" Proceedings of the Association for Information Systems, ed. Young, H. M., August 2000, p.1562-7

Griffin, Jeffrey A. "Electronic Communications vs. Privacy-Can there Be a Balance Between Progress and Individual Rights?" PFIS Track, Proceedings of the Fourth Americas Conference on Information Systems, 1998 Atlanta. p. 832-4

Griffin, Ken and Whitehead, Roy "Privacy in the Age of Technology," International Business and Economics Research Conf. Proceedings on CD-ROM, October 2001 (forthcoming in International Business and Economics Research Journal, accepted December 5, 2001.

Gurak, Laura J. "Professor Takes a Critical Look at Online-Privacy Issues," The Chronicle of Higher Education, March 15, 2002, p. A38.

Hamilton, Richard A. "Privacy Concerns?: Try Enhancement Data," 2001 Hawaii Conference on Business, June 14 -17, 2001. The abstract but not the entire paper, appeared in the CD-ROM Proceedings, file H.doc, p. H-12, Honolulu, Hawaii, USA, Editor(s): Terry Gregson and David Yang.

Helm, Alice K. Everyday Law, Made E-Z Products, Inc., Deerfield Beach, FL, 2000.

Paulson, Linda Dailey. "Key Snooping Technology Causes Controversy," Computer, March 2002, p. 27.

QPB Dictionary of Ideas, New York, New York: Quality Paperback Book Club, 1996, p. 424.